GUTRIDE SAFIER LLP
Seth A. Safier (State Bar No. 197427)
seth@gutridesafier.com
Marie A. McCrary (State Bar No. 262670)
marie@gutridesafier.com
Todd Kennedy (State Bar No. 250267)
todd@gutridesafier.com
Kali R. Backer (State Bar No. 342492)
kali@gutridesafier.com
100 Pine Street, Suite 1250
San Francisco, CA 94111
Telephone: (415) 639-9090
Facsimile: (415) 449-6469

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JONATHAN GABRIELLI, an individual, on behalf of himself, the general public, and those similarly situated,

Plaintiff,

v.

MOTOROLA MOBILITY LLC,

Defendant.

CASE NO.

CLASS ACTION COMPLAINT FOR INVASION OF PRIVACY UNDER CALIFORNIA'S CONSTITUTION; INTRUSION UPON SECLUSION; WIRETAPPING IN VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (CALIFORNIA PENAL CODE § 631); USE OF A PEN REGISTER IN VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (CALIFORNIA PENAL CODE § 638.51); COMMON LAW FRAUD, DECEIT AND/OR MISREPRESENTATION; UNJUST ENRICHMENT; BREACH OF CONTRACT; BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING; AND TRESPASS TO CHATTELS

JURY TRIAL DEMANDED

TABLE OF CONTENTS

INTRODUCTION 3

THE PARTIES 5

JURISDICTION AND VENUE 5

SUBSTANTIVE ALLEGATIONS 5

A. Defendant Programmed the Website to Include Third-Party Resources that Utilize Cookie Trackers. 5

B. Defendant Falsely Informed Users That They Could Reject the Website's Use of Cookies. 10

C. Defendant's Conduct Violated Its Own Privacy Statement. 17

D. The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting Defendant's Website. 18

1. Google Cookies 18

2. TikTok Cookies 23

3. Additional Third Party Cookies 27

E. The Private Communications Collected is Valuable. 28

PLAINTIFF'S EXPERIENCES 29

CLASS ALLEGATIONS 32

CAUSES OF ACTION 34

First Cause of Action: Invasion of Privacy 34

Second Cause of Action: Intrusion Upon Seclusion 36

Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy Act (California Penal Code § 631) 38

Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of Privacy Act (California Penal Code § 638.51) 43

Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation 45

Sixth Cause of Action: Unjust Enrichment 47

Seventh Cause of Action: Breach of Contract 48

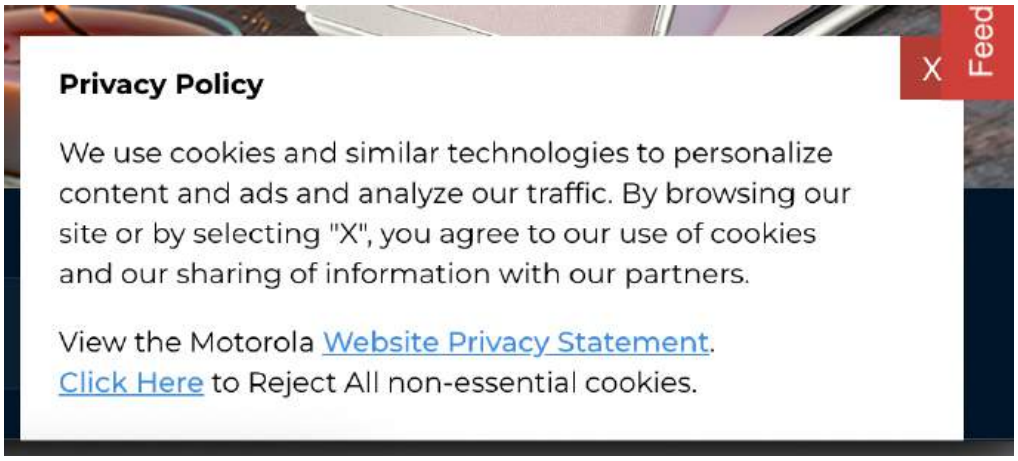
Eighth Cause of Action: Breach of Implied Covenant of Good Faith and Fair Dealing 50

Ninth Cause of Action: Trespass to Chattels 52

Plaintiff Jonathan Gabrielli ("Plaintiff") brings this action on behalf of himself, the general public, and all others similarly situated against Motorola Mobility LLC ("Defendant" or "Motorola"). Plaintiff's allegations against Defendant are based upon information and belief and upon investigation of Plaintiff's counsel, except for allegations specifically pertaining to Plaintiff, which are based upon Plaintiff's personal knowledge.

INTRODUCTION

1. This Class Action Complaint concerns an egregious privacy violation and total breach of consumer trust in violation of California law. When consumers visit Defendant's ecommerce website (www.motorola.com, the "Website"), Defendant displays to them a popup cookie consent banner. Defendant's cookie banner discloses that the Website uses cookies but expressly gives users the option to control how they are tracked and how their personal data is used. Defendant assures visitors that they can choose to "Reject All non-essential cookies" as shown in the following screenshot:



2. Like most internet websites, Defendant designed the Website to include resources and programming scripts from third parties that enable those parties to place cookies and other similar tracking technologies on visitors' browsers and devices and/or transmit cookies along with user data. However, unlike other websites, Defendant's Website offers consumers a choice to browse without being tracked, followed, and targeted by third party data brokers and advertisers. However, Defendant's promises are outright lies, designed to lull users into a false sense of security. Even after users elect to "Reject All non-essential cookies", Defendant

surreptitiously enables several third parties – including Google LLC (DoubleClick and Google Analytics), ByteDance Ltd. (TikTok), Amazon.com, Inc. (amazon-adsystem), Howl Technologies, Inc. (Narrativ), and Emplifi, Inc. (GoInStore) (the "Third Parties") – to place and/or transmit cookies that track users' website browsing activities and eavesdrop on users' private communications on the Website.

3. Contrary to their express rejection of cookies and tracking technologies on the Website, Defendant nonetheless caused cookies, including the Third Parties' cookies, to be sent to Plaintiff and other visitors' browsers, stored on their devices, and transmitted to the Third Parties along with user data. These third-party cookies permitted the Third Parties to track and collect data in real time regarding Website visitors' behaviors and communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

4. The Third Parties analyze and aggregate this user data across websites and time for their own purposes and financial gain, including, creating consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics; creating audience segments based on shared traits (such as millennials, tech enthusiasts, etc.); and performing targeted advertising and marketing analytics. Further, the Third Parties share user data and/or user profiles to unknown parties to further their financial gain.

5. This type of tracking and data sharing is exactly what the Website visitors who clicked or selected the "Reject All" button on the Website's cookie consent banner sought to avoid. Defendant falsely told Website users that it respected their privacy and that they could avoid tracking and data sharing when they browsed the Website. Despite receiving notice of consumers' express declination of consent, Defendant defied it and violated state statutes, tort duties, and also breached its contractual duties and the implied covenant of good faith and fair dealing with Plaintiff and those similarly situated Website users.

THE PARTIES

6. Plaintiff Jonathan Gabrielli is, and was at all relevant times, an individual and resident of Oakland, California. Plaintiff intends to remain in California and makes his permanent home there.

7. Defendant Motorola Mobility LLC is a Delaware limited liability corporation with its headquarters and principal place of business in Illinois.

JURISDICTION AND VENUE

8. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332(d)(2). The aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs; and Plaintiff and Defendant are citizens of different states.

9. The injuries, damages and/or harm upon which this action is based, occurred or arose out of activities engaged in by Defendant within, affecting, and emanating from, the State of California. Defendant regularly conducts and/or solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products and services provided to persons in the State of California. Defendant has engaged, and continues to engage, in substantial and continuous business practices in the State of California.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in the state of California, including within this District.

11. Plaintiff accordingly alleges that jurisdiction and venue are proper in this Court.

SUBSTANTIVE ALLEGATIONS

A. Defendant Programmed the Website to Include Third-Party Resources that Utilize Cookie Trackers.

12. Every website, including the Website, is hosted by a server that sends and receives communications in the form of HTTP requests, such as "GET" or "POST" requests, to and from Internet users' browsers. For example, when a user clicks on a hyperlink on the Website, the user's browser sends a "GET" request to the Website's server. The GET request tells the Website server what information is being requested (e.g., the URL of the webpage being

requested) and instructs the Website's server to send the information back to the user (e.g., the content of the webpage being requested). When the Website server receives an HTTP request, it processes that request and sends back an HTTP response. The HTTP request includes the client's IP address so that the Website server to knows where to send the HTTP response.

13. An IP address (Internet Protocol address) is a unique numerical label assigned to each device connected to a network that uses the Internet Protocol for communication, typically expressed as four sets of numbers separated by periods (e.g., 192.168.123.132 for IPv4 addresses). IP addresses can identify the network a device is on and the specific device within that network. Public IP addresses used for internet-facing devices reveal geographical locations, such as country, city, or region, through IP geolocation databases.

14. Defendant voluntarily integrated "third-party resources" from the Third Parties into its Website programming. "Third-party resources" refer to tools, content or services provided by third-parties, such as analytics tools, advertising networks, or payment processors, that a website developer utilizes by embedding scripts, styles, media, or application programming interface (API) into the website's code. Defendant's use of the third-party resources on the Website is done so pursuant to agreements between Defendant and those Third Parties.

15. The Website causes users' devices to store and/or transmit both first-party and third-party tracking cookies. Cookies are small text files sent by a website server to a user's web browser and stored locally on the user's device. As described below, cookies generally contain a unique identifier which enables the website to recognize and differentiate individual users. Cookie files are sent back to the website server along with HTTP requests, enabling the website to identify the device making the requests, and to record a session showing how the user interacts with the website.

16. First-party cookies are those that are placed on the user's device directly by the web server with which the user is knowingly communicating (in this case, the Website's server). First-party cookies are used to track users when they repeatedly visit the same website.

17. A third-party cookie is set by a third-party domain/webserver (e.g., www.google.com; td.doubleclick.net; s.amazon-adsystem.com; analytics.tiktok.com, etc.). When the user's browser loads a webpage (such as a webpage of the Website) containing embedded third-party resources, the third-parties' programming scripts typically issue HTTP commands to determine whether the third-party cookies are already stored on the user's device and to cause the user's browser to store those cookies on the device if they do not yet exist. Third-party cookies include an identifier that allows the third-party to recognize and differentiate individual users across websites (including the Website) and across multiple browsing sessions.

18. As described further below, the third-party cookies stored on and/or loaded from users' devices when they interact with the Website are transmitted to those third parties, enabling them to surreptitiously track in real time and collect Website users' personal information, such as their browsing activities and private communications with Defendant, including the following:

- **Browsing History**: Information about the webpages a Website user visits, including the URLs, titles, and keywords associated with the webpages viewed, time spent on each page, and navigation patterns;
- **Visit History**: Information about the frequency and total number of visits to the Website;
- **Website Interactions:** Data on which links, buttons, or ads on the Website that a user clicks;
- **User Input Data**: The information the user entered into the Website's form fields, including search queries, the user's name, age, gender, email address, location, and/or payment information;
- **Demographic Information**: Inferences about age, gender, and location based on browsing habits and interactions with Website content;
- **Interests and Preferences**: Insights into user interests based on the types of Website content viewed, products searched for, or topics engaged with;

- **Shopping Behavior**: Information about the Website products viewed or added to shopping carts;
- **Device Information**: Details about the Website user's device, such as the type of device (mobile, tablet, desktop), operating system, and browser type;
- **Referring URL**: Information about the website that referred the user to the Website;
- **Session Information**: Details about the user's current Website browsing session, including the exact date and time of the user's session, the session duration and actions taken on the Website during that session;
- **User Identifiers**: A unique ID that is used to recognize and track a specific Website user across different websites over time; and/or
- **Geolocation Data**: General location information based on the Website user's IP address or GPS data, if accessible.

(Collectively, the browsing activities and private communications listed in the bullet points above shall be referred to herein as "Private Communications").

19. Third-party cookies can be used for a variety of purposes, including (i) analytics (e.g., tracking and analyzing visitor behavior, user engagement, and effectiveness of marketing campaigns); (ii) personalization (e.g., remembering a user's browsing history and purchase preferences to enable product recommendations); (iii) advertising/targeting (e.g., delivering targeted advertisements based on the user's consumer profile (i.e., an aggregated profile of the user's behavior, preferences, and demographics); and (iv) social media integration (e.g., enabling sharing of users' activities with social media platforms). Ultimately, third-party cookies are utilized to boost website performance and revenue through the collection, utilization, and dissemination of user data.

20. Defendant specializes in consumer electronics, primarily manufacturing smartphones and mobile devices. Defendant owns and operates the Website, which allows visitors to receive information about its products and purchase products. As they interact with

the Website (e.g., by entering data into forms, clicking on links, and making selections), Website users communicate Private Communications to Defendant, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

21. Defendant chose to install or integrate its Website with resources from the Third Parties that, among other things, use cookies. Thus, when consumers visit the Website, both first-party cookies and third-party cookies are placed on their devices and/or transmitted. This is caused by software code that Defendant incorporates into its Website, or that Defendant causes to be loaded. Because Defendant controls the software code of its Website, it has complete control over whether first-party and third-party cookies are placed on its users' devices and/or transmitted to third parties.

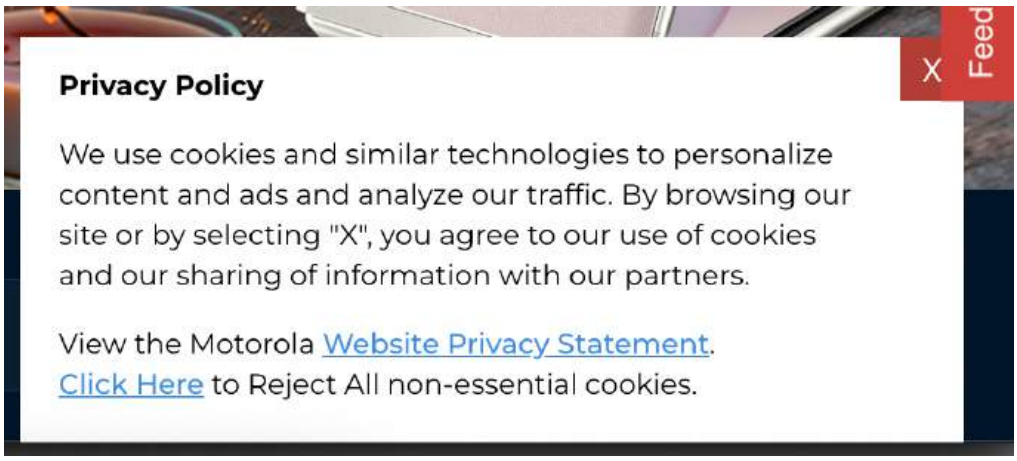
22. Defendant explained the third-party cookies it used on the Website as follows in its privacy statement:

> We also use cookies and ad pixels (a piece of code) to determine relevant interest-based advertisements to serve the user. For this purpose, Motorola may use services hosted by companies such as Google Analytics for Display Advertisers, Remarketing with Google Analytics, Google Display Network Impression Reporting, DoubleClick Campaign Manager and Google Analytics Demographic and Interest Reporting, Facebook, Snapchat, and Tiktok to help us understand our customers' use of our websites and products; to match certain data about our customers, uses of our websites, and social media engagement; and to deliver and manage interest-based advertisements. These services may collect information, such as an IP address, sent by your browser or via cookies. Motorola may also share certain limited (often hashed) information with our ad partners so that they may provide these services to Motorola.
>
> In addition, cookies, pixels, and related technologies allow us to measure website trends and traffic patterns, such as which areas of the Motorola site you visited and which site you came from (including via session replay analytics tools); to reduce customer frustration and simplify site navigation; to help design our site to make it more efficient and enjoyable; to make product recommendations; to deliver a Motorola product advertisement while browsing a website including on non-Motorola websites, and to prevent fraud. Motorola and its service providers, including Google and DoubleClick, use cookies to report how your ad impressions, other uses of ad services, and interactions with these ad impressions and ad services are related to visits to our website. … Motorola may also supplement information

collected via cookies and related technologies with information acquired from other sources, including third parties.[1]

B. Defendant Falsely Informed Users That They Could Reject the Website's Use of Cookies.

23. When consumers in California visited the Website, the Website immediately displayed to them a popup cookie consent banner. As shown in the screenshot below, the cookie consent banner stated, "We use cookies and similar technologies to personalize content and ads and analyze our traffic. By browsing our site or by selecting "X", you agree to our use of cookies and our sharing of information with our partners." The banner then purported to provide users the opportunity to "Click Here to Reject All non-essential cookies" as shown, in the following screenshot from the Website:



24. Website users who clicked or selected the "Click Here to Reject All non-essential cookies" link, indicating their choice and/or agreement to decline or reject all cookies and tracking technologies in use on the Website, could then continue to browse the Website, and the popup cookie consent banner disappeared.

25. Defendant's popup cookie consent banner led Plaintiff, and all those Website users similarly situated, to believe that they declined or rejected all cookies and tracking technologies, especially those that used to "personalize content and ads and analyze [Website]

[1] Motorola Mobility Website Privacy Statement (updated 5/1/2023) (available at https://help.motorola.com/hc/apps/privacy/web/2023-05/en-us/) (the "Privacy Statement"). Defendant has subsequently updated its Privacy Statement but, based on information and belief, this version was in effect at the time of Plaintiff's rejection of cookies on the Website.

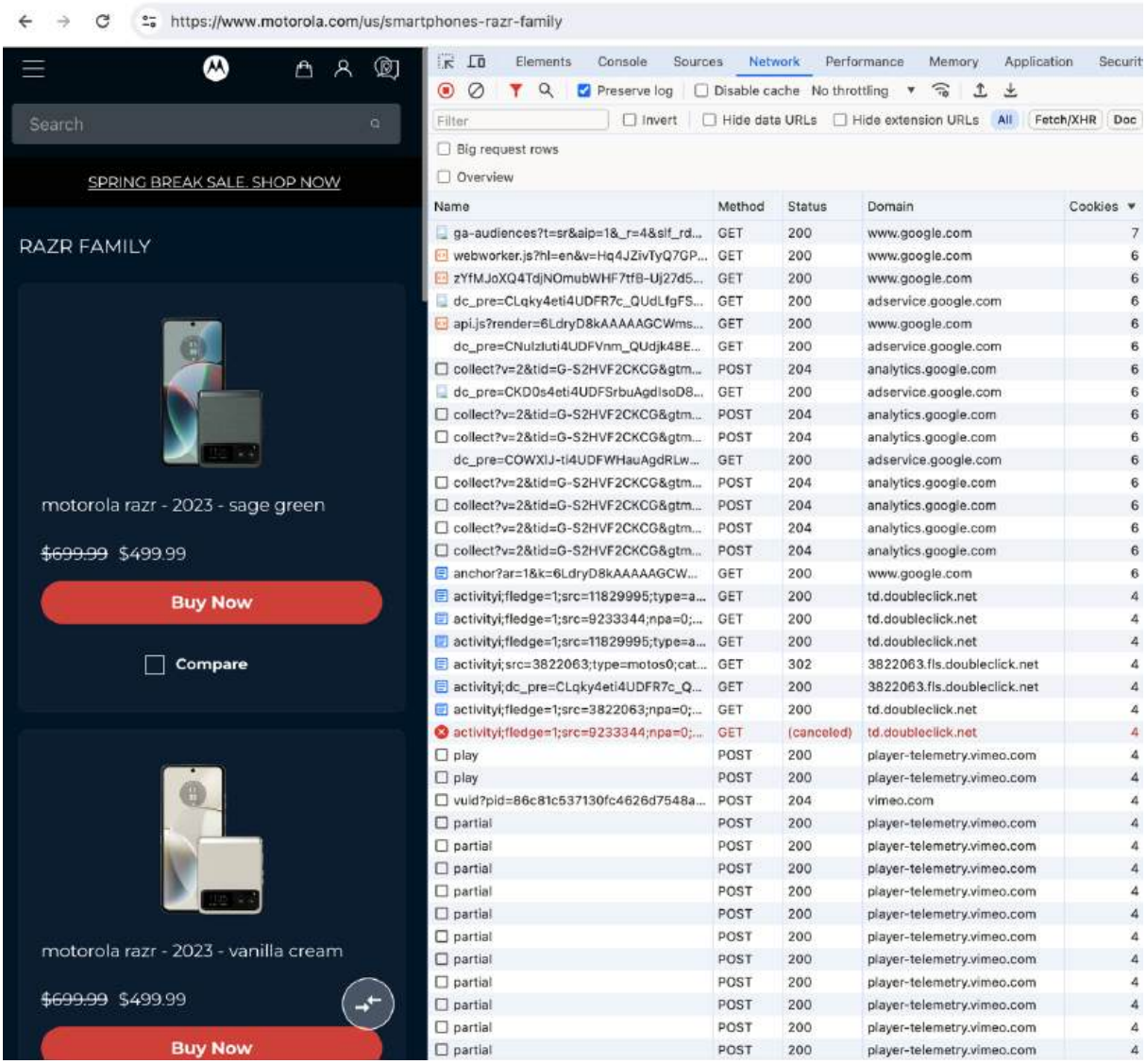
traffic." The banner further reasonably led Plaintiff and those Website users similarly situated to believe that Defendant would not allow third parties, through cookies, to access their Private Communications with the Website, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, upon clicking or selecting the "Click Here to Reject All non-essential cookies" link.

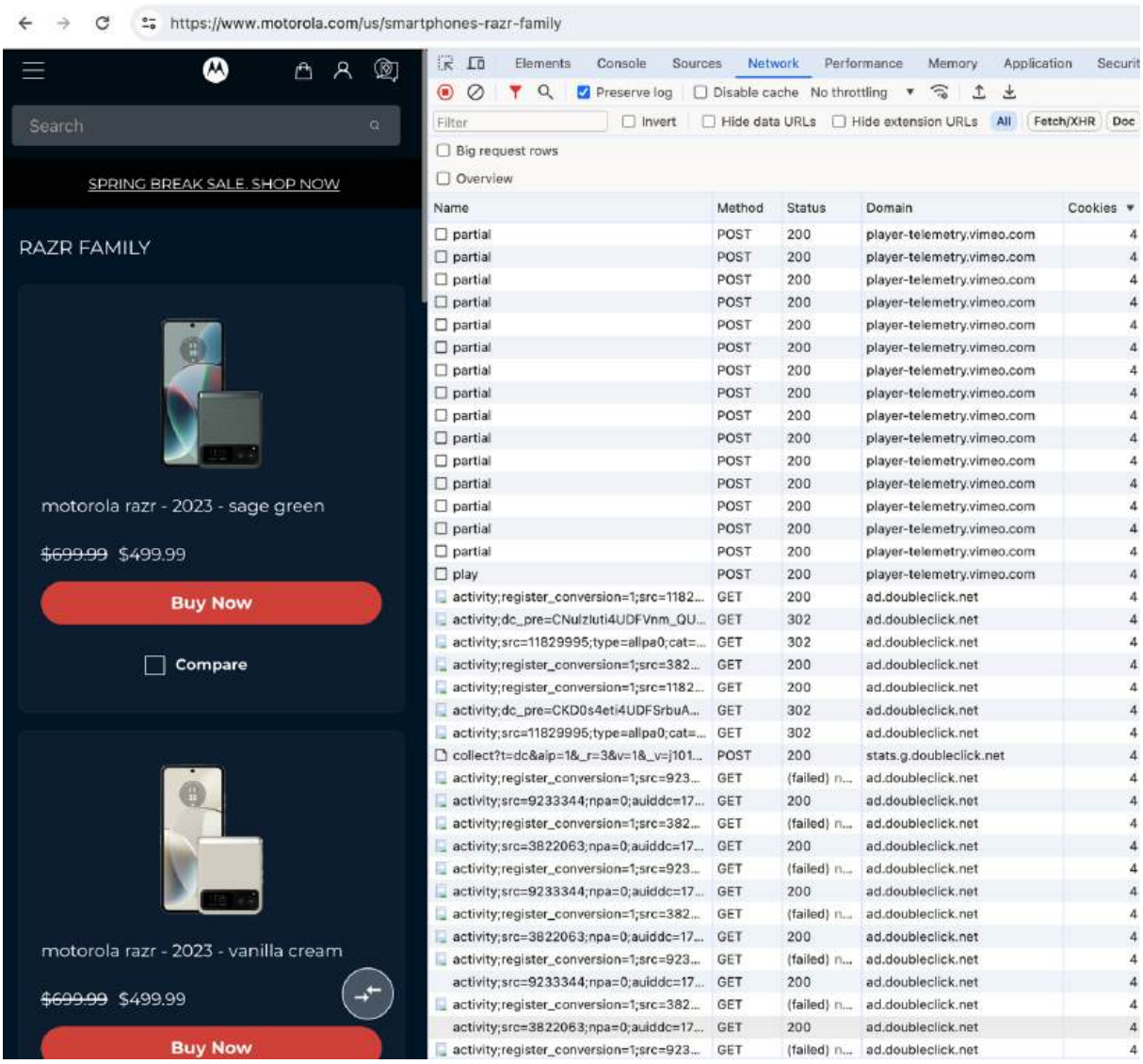
26. Defendant's representations, however, were false. In truth, Defendant did not abide by its users' wishes. When users clicked the "Click Here to Reject All non-essential cookies" link, they provided notice to Defendant that they did not consent to the placement or transmission of third-party cookies that would allow those parties to obtain their Private Communications with the Website. Nevertheless, Defendant caused the Third Party tracking cookies to be placed on Website users' browsers and devices and/or transmitted to the Third Parties along with user data.

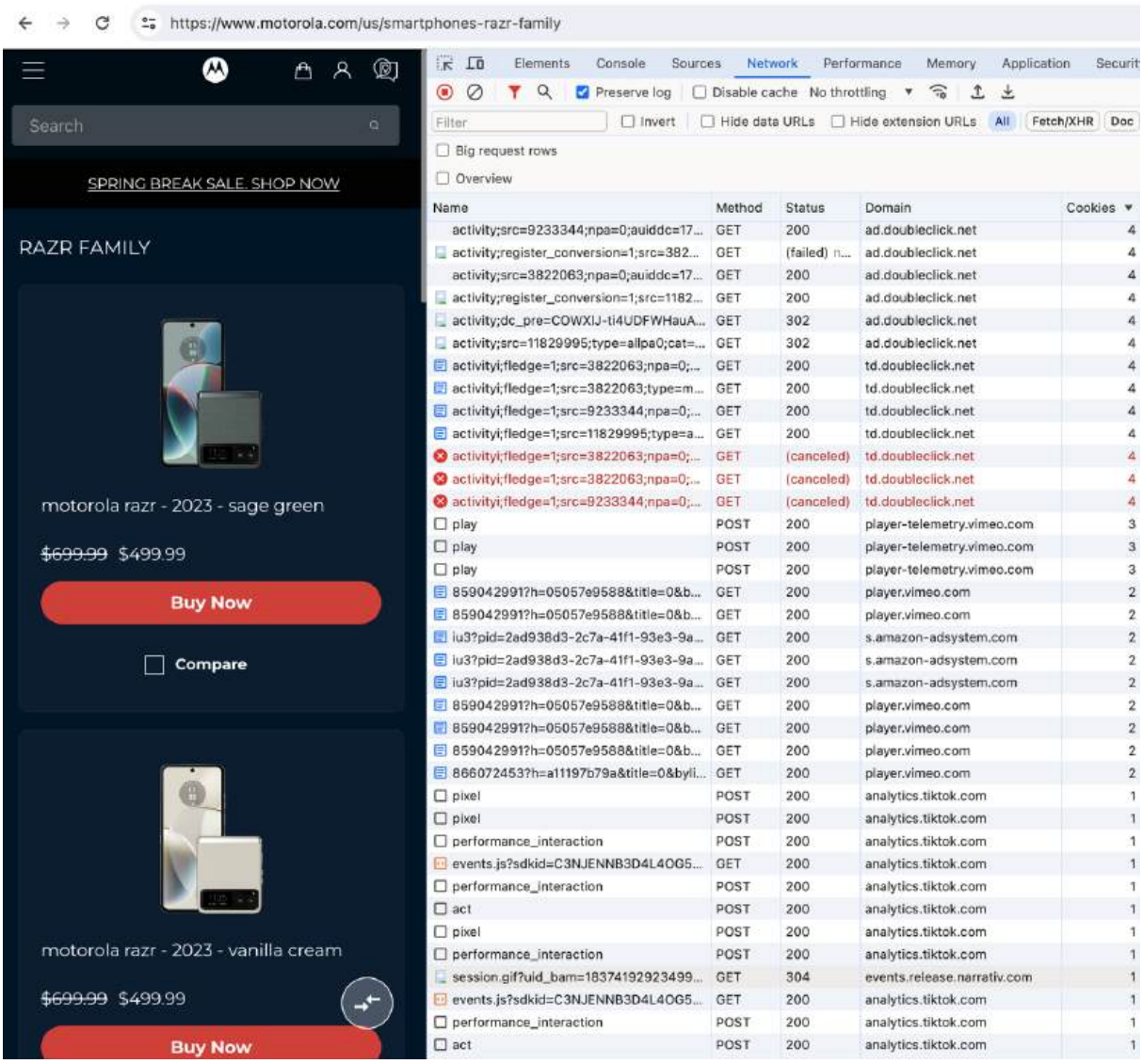
27. In particular, when users clicked or selected the "Click Here to Reject All non-essential cookies" link, Defendant nonetheless continued to cause the Third Parties' cookies to be placed on users' devices and/or transmitted to the Third Parties along with user data, enabling them to collect user data in real time that discloses Website visitors' Private Communications, including browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data. In other words, even when consumers like Plaintiff tried to protect their privacy by rejecting cookies, Defendant failed to prevent cookies from being transmitted to Third Parties, enabling them to track user behavior and communications.

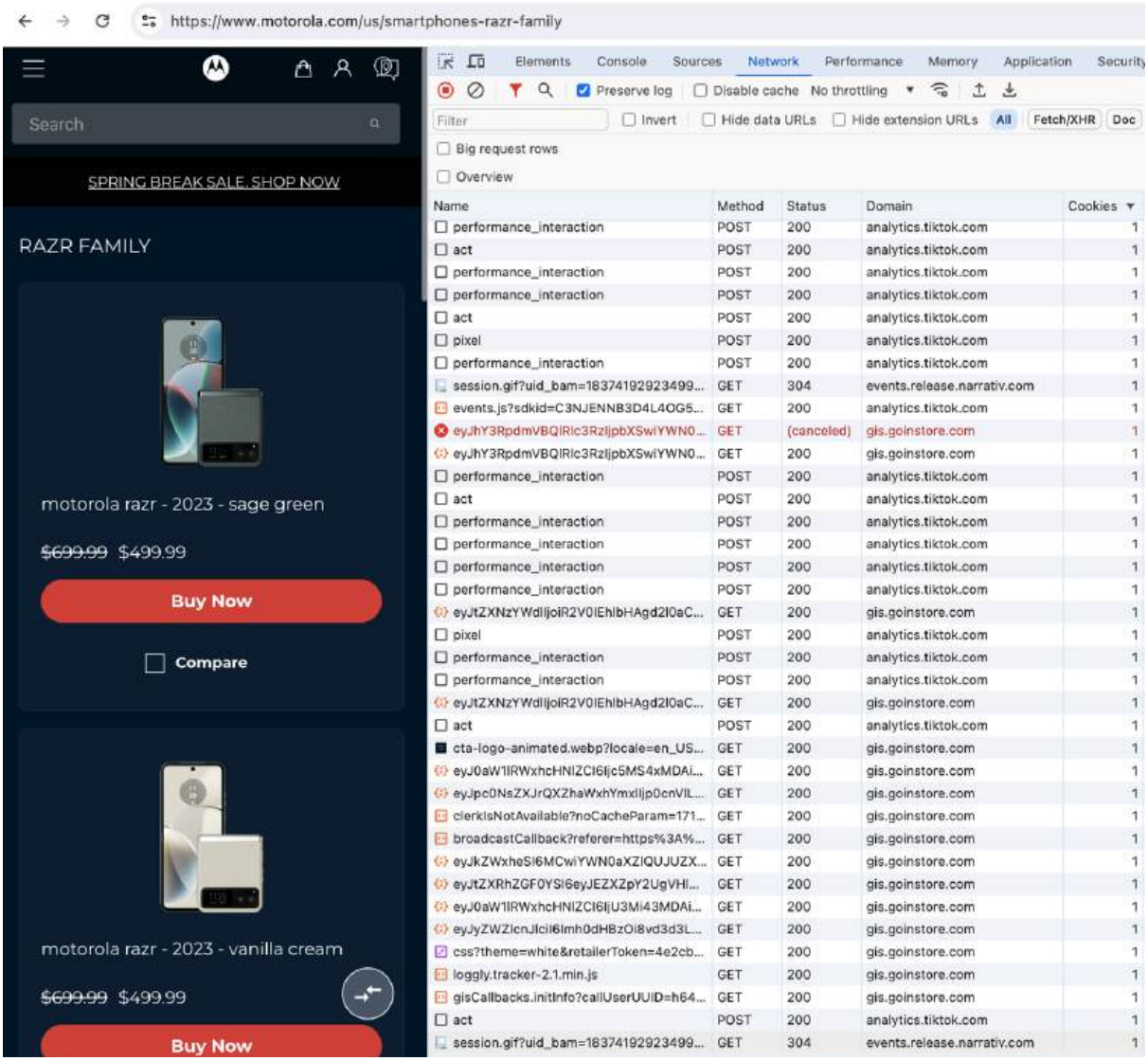
28. Some aspects of the operations of the Third Party cookies on the Website can be observed using specialized tools that log incoming and outgoing Website network transmissions. The following screenshots, obtained using one such tool, show examples of Third-Party cookies

being transmitted from a Website user's device and browser to Third Parties even after the user clicked the "Click Here to Reject All non-essential cookies" link on the Website's popup cookie consent banner.




https://www.motorola.com/us/smartphones-razr-family
Search
SPRING BREAK SALE. SHOP NOW
RAZR FAMILY
motorola razr - 2023 - sage green
$699.99 $499.99
Buy Now
Compare
motorola razr - 2023 - vanilla cream
$699.99 $499.99
Buy Now
Elements Console Sources Network Performance Memory Application Securit
Preserve log Disable cache No throttling
Filter Invert Hide data URLs Hide extension URLs All Fetch/XHR Doc
Big request rows
Overview
Name Method Status Domain Cookies
partial POST 200 player-telemetry.vimeo.com 4
play POST 200 player-telemetry.vimeo.com 4
activity;register_conversion=1;src=1182... GET 200 ad.doubleclick.net 4
activity;dc_pre=CNulzluti4UDFVnm_QU... GET 302 ad.doubleclick.net 4
activity;src=11829995;type=allpa0;cat=... GET 302 ad.doubleclick.net 4
activity;register_conversion=1;src=382... GET 200 ad.doubleclick.net 4
activity;register_conversion=1;src=1182... GET 200 ad.doubleclick.net 4
activity;dc_pre=CKD0s4eti4UDFSrbuA... GET 302 ad.doubleclick.net 4
activity;src=11829995;type=allpa0;cat=... GET 302 ad.doubleclick.net 4
collect?t=dc&aip=1&_r=3&v=1&_v=j101... POST 200 stats.g.doubleclick.net 4
activity;register_conversion=1;src=923... GET (failed) n... ad.doubleclick.net 4
activity;src=9233344;npa=0;auiddc=17... GET 200 ad.doubleclick.net 4
activity;register_conversion=1;src=382... GET (failed) n... ad.doubleclick.net 4
activity;src=3822063;npa=0;auiddc=17... GET 200 ad.doubleclick.net 4
activity;register_conversion=1;src=923... GET (failed) n... ad.doubleclick.net 4
activity;src=9233344;npa=0;auiddc=17... GET 200 ad.doubleclick.net 4
activity;register_conversion=1;src=382... GET (failed) n... ad.doubleclick.net 4
activity;src=3822063;npa=0;auiddc=17... GET 200 ad.doubleclick.net 4
activity;register_conversion=1;src=923... GET (failed) n... ad.doubleclick.net 4
activity;src=9233344;npa=0;auiddc=17... GET 200 ad.doubleclick.net 4
activity;register_conversion=1;src=382... GET (failed) n... ad.doubleclick.net 4
activity;src=3822063;npa=0;auiddc=17... GET 200 ad.doubleclick.net 4
activity;register_conversion=1;src=923... GET (failed) n... ad.doubleclick.net 4


https://www.motorola.com/us/smartphones-razr-family
Search
SPRING BREAK SALE. SHOP NOW
RAZR FAMILY
motorola razr - 2023 - sage green
$699.99 $499.99
Buy Now
Compare
motorola razr - 2023 - vanilla cream
$699.99 $499.99
Buy Now
Elements Console Sources Network Performance Memory Application Securit
Preserve log Disable cache No throttling
Filter Invert Hide data URLs Hide extension URLs All Fetch/XHR Doc
Big request rows
Overview
Name Method Status Domain Cookies
activity;src=9233344;npa=0;auiddc=17... GET 200 ad.doubleclick.net 4
activity;register_conversion=1;src=382... GET (failed) n... ad.doubleclick.net 4
activity;src=3822063;npa=0;auiddc=17... GET 200 ad.doubleclick.net 4
activity;register_conversion=1;src=1182... GET 200 ad.doubleclick.net 4
activity;dc_pre=COWXIJ-ti4UDFWHauA... GET 302 ad.doubleclick.net 4
activity;src=11829995;type=allpa0;cat=... GET 302 ad.doubleclick.net 4
activityi;fledge=1;src=3822063;npa=0;... GET 200 td.doubleclick.net 4
activityi;fledge=1;src=3822063;type=m... GET 200 td.doubleclick.net 4
activityi;fledge=1;src=9233344;npa=0;... GET 200 td.doubleclick.net 4
activityi;fledge=1;src=11829995;type=a... GET 200 td.doubleclick.net 4
activityi;fledge=1;src=3822063;npa=0;... GET (canceled) td.doubleclick.net 4
activityi;fledge=1;src=3822063;npa=0;... GET (canceled) td.doubleclick.net 4
activityi;fledge=1;src=9233344;npa=0;... GET (canceled) td.doubleclick.net 4
play POST 200 player-telemetry.vimeo.com 3
play POST 200 player-telemetry.vimeo.com 3
play POST 200 player-telemetry.vimeo.com 3
859042991?h=05057e9588&title=0&b... GET 200 player.vimeo.com 2
859042991?h=05057e9588&title=0&b... GET 200 player.vimeo.com 2
iu3?pid=2ad938d3-2c7a-41f1-93e3-9a... GET 200 s.amazon-adsystem.com 2
iu3?pid=2ad938d3-2c7a-41f1-93e3-9a... GET 200 s.amazon-adsystem.com 2
iu3?pid=2ad938d3-2c7a-41f1-93e3-9a... GET 200 s.amazon-adsystem.com 2
859042991?h=05057e9588&title=0&b... GET 200 player.vimeo.com 2
859042991?h=05057e9588&title=0&b... GET 200 player.vimeo.com 2
859042991?h=05057e9588&title=0&b... GET 200 player.vimeo.com 2
866072453?h=a11197b79a&title=0&byli... GET 200 player.vimeo.com 2
pixel POST 200 analytics.tiktok.com 1
pixel POST 200 analytics.tiktok.com 1
performance_interaction POST 200 analytics.tiktok.com 1
events.js?sdkid=C3NJENNB3D4L4OG5... GET 200 analytics.tiktok.com 1
performance_interaction POST 200 analytics.tiktok.com 1
act POST 200 analytics.tiktok.com 1
pixel POST 200 analytics.tiktok.com 1
performance_interaction POST 200 analytics.tiktok.com 1
session.gif?uid_bam=18374192923499... GET 304 events.release.narrativ.com 1
events.js?sdkid=C3NJENNB3D4L4OG5... GET 200 analytics.tiktok.com 1
performance_interaction POST 200 analytics.tiktok.com 1
act POST 200 analytics.tiktok.com 1



29. The screenshots above show the "Network" tab of Chrome Developer Tools, which contains a list of HTTP network traffic transmissions between the user's browser and various third party websites while the user visited and interacted with Defendant's Website at https://www.motorola.com. The screenshots depict only network traffic occurring ***after*** the user rejected all cookies using the cookie banner. As shown above, despite the user's rejection of all cookies, the user's interactions with the Website resulted in the user's browser making a large number of GET and POST HTTP requests to third party web domains like ad.doubleclick.net, analytics.tiktok.com, and others. As further shown in the right-hand column of the screenshots, the user's browser sent cookies along with those HTTP requests to the third parties. These screenshots demonstrate that the Website caused third-party cookie data and

users' Private Communications to be transmitted to Third Parties, even after consumers declined or rejected all cookies and tracking technologies by clicking or selecting the "Click Here to Reject All non-essential cookies" link. All of these network calls are made to the Third Parties without the user's knowledge, and despite the user's rejection of all cookies.

30. Website users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, are surreptitiously obtained by the Third Parties via these cookies.

31. As users interact with the Website, even after clicking or selecting the "Click Here to Reject All non-essential cookies" link, thereby declining or rejecting the use of cookies and similar technologies for personalized content, advertising, and analytics, as well as the sale or sharing of the user's personal information with third parties for such functions, or other purposes, more data regarding users' behavior and communications are sent to third parties, alongside the cookie data. The third-party cookies that Defendant wrongfully allows to be stored on users' devices and browsers, and to be transmitted to the Third Parties, enable the Third Parties to track and collect data on users' behaviors and communications, including Private Communications, on the Website. Because third-party cookies enable Third Parties to track users' behavior across the Internet and across time, user data can be correlated and combined with other data sets to compile comprehensive user profiles that reflect consumers' behavior, preferences, and demographics (including psychological trends, predispositions, attitudes, intelligence, abilities, and aptitudes). These Third Parties monetize user profiles for advertising, sales, and marketing purposes to generate revenue and target advertising to Internet users. Advertisers can gain deep understanding of users' behavioral traits and characteristics and target those users with advertisements tailored to their consumer profiles and audience segments.

32. The Third Party code that the Website causes to be loaded and executed by the user's browser becomes a wiretap when it is executed because it enables the Third Parties—

separate and distinct entities from the parties to the conversations—to use cookies to eavesdrop upon, record, extract data from, and analyze conversations to which they are not parties. When the Third Parties use their respective wiretaps on Website users' Private Communications, the wiretaps are not like tape recorders or "tools" used by one party to record the other. The Third Parties each have the capability to use the contents of conversations they collect through their respective wiretaps for their own purposes as described in more detail below.

C. Defendant's Conduct Violated Its Own Privacy Statement.

33. Defendant's aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties to track users' Private Communications on the Website using third-party cookies—even after those users click or select the "Click Here to Reject All non-essential cookies" link—is particularly egregious given Defendant's additional written assurances in its Privacy Statement that users can, in fact, opt out of cookies and tracking technologies used on the Website. Specifically, Defendant represented to Plaintiff and its users the following in the Privacy Statement:

> Where required by applicable law, Motorola will acquire consent from you prior to using certain cookies during your Motorola website experience and/or will offer you the opportunity to choose which types of cookies to enable or disable.
>
> ...
>
> Motorola and its service providers, including Google and DoubleClick, use cookies to report how your ad impressions, other uses of ad services, and interactions with these ad impressions and ad services are related to visits to our website. If you do not want to have this information used for serving you interest-based ads, you may opt-out by following the steps below.
> ...
>
> However, if you prefer not to store cookies, you can choose to...Utilize the cookie consent and control options offered by a Motorola website (if available and as required by applicable law)[.]

Privacy Statement.

D. The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting Defendant's Website.

1. Google Cookies

34. Defendant causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users reject all non-essential cookies (including advertising and analytics cookies) to and from the **www.google.com, adservice.google.com, analytics.google.com, and doubleclick.net** domains. Each of these domains is associated with Google LLC's digital advertising and analytics platform that collects user information via cookies to assist Google in performing data collection, behavioral analysis, user retargeting, and analytics.[2] Google serves targeted ads to web users across Google's ad network, which spans millions of websites and apps. Nearly 20% of web traffic is tracked by Google's DoubleClick cookies.[3] Google's cookies help it track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. Further, by identifying users who have shown interest in certain products or content, Google's cookies enable its advertising platform to enable advertisers to show relevant ads to those users when they visit other websites within Google's ad network.[4]

35. Specifically, Google sends cookies when a web user visits a webpage that shows Google Marketing Platform advertising products and/or Google Ad Manager ads.[5] "Pages with Google Marketing Platform advertising products or Google Ad Manager ads include ad tags that

---

[2] *See* Our advertising and measurement cookies (available at https://business.safety.google/adscookies/).

[3] *See, e.g.* https://www.ghostery.com/whotracksme/trackers/doubleclick.

[4] *See, e.g.* About cross-channel remarketing in Search Ads 360 (available at https://support.google.com/searchads/answer/7189623?hl=en); About dynamic remarketing for retail (available at https://support.google.com/google-ads/answer/6099158?hl=en&sjid=11962135750754589 08-NC).

[5] *See* How Google Marketing Platform advertising products and Google Ad Manager use cookies (available at https://support.google.com/searchads/answer/2839090?hl=en&sjid=11962135750754589 08-NC); *see also* Cookies and user identification (available at https://developers.google.com/tag-platform/security/concepts/cookies).

instruct browsers to request ad content from [Google's] servers. When the server delivers the ad content, it also sends a cookie. But a page doesn't have to show Google Marketing Platform advertising products or Google Ad Manager ads for this to happen; it just needs to include Google Marketing Platform advertising products or Google Ad Manager ad tags, which might load a click tracker or impression pixel instead." *Id.* As Google explains, "Google Marketing Platform advertising products and Google Ad Manager send a cookie to the browser after any impression, click, or other activity that results in a call to our servers." *Id.*

36. Google also uses cookies in performing analytical functions. As Google explains, "Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights into [] business[es]."[6] "To measure a website … [one] add[s] a small piece of JavaScript measurement code to each page on [a] site." *Id.* Then, "[e]very time a user visits a webpage, the tracking code will collect … information about how that user interacted with the page." *Id.* Google Analytics enables website owners to "measure when someone loads a page, clicks a link, [ ] makes a purchase;" "completes a purchase"; "searches [] website or app"; "select content on [] website or app"; "views an item"; and "views their shopping cart."[7]

37. Google's cookies allow it to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data.[8]

---

[6] How Google Analytics Works (available at https://support.google.com/analytics/answer/12159447?hl=en).

[7] Set up events (available at https://developers.google.com/analytics/devguides/collection/ga4/events); and Recommended events (available at https://developers.google.com/analytics/devguides/collection/ga4/events).

[8] *See* About the Google Tag (available at https://support.google.com/searchads/answer/7550511?hl=en); How Floodlight Recognizes Users (available at https://support.google.com/searchads/answer/2903014?hl=en); How Google Ads tracks website conversions (available at https://support.google.com/google-ads/answer/7521212);

38. For example, the Google software code that Defendant causes to be stored on and executed by the Website user's device causes the following data to be sent to Google's domain, at https://www.google.com/ads/ga-audiences:

Key	Value
t	sr
aip	1
_r	4
slf_rd	1
v	1
_v	j101
tid	UA-29445500-1
cid	464953708.1707536935
jid	1670887984
_u	yCCAAUACQAAAACAAI~
z	205787557

39. The "cid" cookie above refers to "Client ID." It contains a unique identifier for a the user's browser and device, that enables Google to link the user to their interactions with the website.[9] The "jid" is the "JoinID," which binds the Google Analytics cookie to the cookie for DoubleClick, which is Google's advertising platform. *Id.*

40. Along with this data, the Google software code that Defendant causes to be stored on and executed by the user's device causes the following cookies to be sent to Google's domain:

Google Ads Help, Cookie: Definition (available at https://support.google.com/google-ads/answer/2407785?hl=en); About demographic targeting in Google Ads (available at https://support.google.com/searchads/answer/7298581?hl=en&sjid=1196213575075458908-NC&visit_id=638670675669576522-2267083756&ref_topic=7302618&rd=1); How Google Analytics Works (https://support.google.com/analytics/answer/12159447); Set up events (available at https://developers.google.com/analytics/devguides/collection/ga4/events); and Recommended events (available at https://support.google.com/analytics/answer/9267735).

[9] *See, e.g.*, https://cheatography.com/dmpg-tom/cheat-sheets/google-universal-analytics-url-collect-parameters/; https://www.analyticsmarket.com/blog/how-google-analytics-collects-data/; https://www.owox.com/blog/use-cases/google-analytics-client-id/

Key	Value
__Secure-3PSID	g.a000gAiz-gjcy9PxUkGPEloXrgm0KsFceRZBRjTapp2rXUEjmbV6-ii6B75iCYV5cZNWZtV3JgACgYKAV8SAQASFQHGX2Mit_7WfQ6Molj-FhX_y2QnBBoVAUF8yKr3kp_8v3R924GKid97okLB0076
__Secure-3PAPISID	xc2d-En2rCSl4sLZ/AzurvDbFWo34MEY-h
NID	511=tL5XKddaFXqqJqasnk_ve17dvcv4N0Zq2wHiFsDT4-szkqL_LrBcZLRX3y1C0B0Z9kUvFobjAEEoEW_o-NaG46f4UJC493H4bZlMbaRtFQRQ3S5k61LSjZpjgNeMn1wfhZDErttflHKzWz71l7qlMQlmib-FJXtE6cZjcPz2nDHLMnf7MrfXGlsJVbpm3M21AyXPel3mGhsMOsPqMcOt0YtKZe1_pvf1u_Zz25N_LS06ngdxLWMPXNKtVfN1pGynQ9oOw-ZBjZchRuCkkynX9ctPeNvOXdviHnJlrR6Qurk
1P_JAR	2024-02-10-03
__Secure-3PSIDTS	sidts-CjIBPVxjSgLm4VkM8OKr_uu39fFduoJCrvrm7BcdbR91v8TU1DA3gK5Wy9lbfRYDFo7e-RAA
__Secure-3PSIDCC	ABTWhQGNkvDDI1pDBgxe8ifi4DaWIQsCJ6XAddK9ad9F0JxwKr7KyTDW6KhFBnqSMHMXrZZ2ag

41. The __Secure-3PAPISID, __Secure-3PSID, and __Secure-APISID cookies used on the Website are utilized by Google to build a profile of Website visitor interests to show relevant and personalized ads through retargeting.

42. Further, along with all of this data, the Google software code that Defendant causes to be stored on and executed by the user's device causes the user's "user-agent" information to be sent to Google:

Key	Value
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

43. The "user-agent" corresponds to the device and browser that the user has used to access the Website. In this case, the user-agent value corresponds to Google's Chrome browser version 121, running on the Catalina version of macOS.[10]

44. Finally, the data sent to Google contains the user's IP address.

[10] There are many tools on the web that are capable of parsing user-agent strings to determine what browser and operating system they pertain to. One such tool is located at https://explore.whatismybrowser.com/useragents/parse.

45. Because Google's cookies operate across multiple sites (i.e., cross-site tracking), the cookie enables Google to track users as they navigate from one site to another, and to comprehensively observe and evaluate user behavior online. Google's advertising platform aggregates user data to create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics and audience segments based on shared traits (such as females, Millennials, etc.), and to perform targeted advertising and marketing analytics.

46. Thus, the Google cookies used on the Website enable Google to track users' interactions with advertisements to help advertisers understand how users engage with ads across different websites. Further, the user data collected through the cookie enables the delivery of personalized ads based on user interests and behaviors. For instance, if a user frequently visits travel-related websites, Google will show her more travel-related advertisements. Further, the collected data is used to generate reports for advertisers, helping them assess the performance of their ad campaigns and make data-driven decisions (such as renaming their products). Further, Google's advertising platform enables advertisers to retarget marketing, which Google explains allows advertisers to "show previous visitors ads based on products or services they viewed on your website. With messages tailored to your audience, dynamic remarketing helps you build leads and sales by bringing previous visitors back to your website to complete what they started."[11]

47. Further, in its "Shared Data Under Measurement Controller-Controller Data Protection Terms," Google states: "Google can access and analyze the Analytics data customers share with us to better understand online behavior and trends, and improve our products and services—for example, to improve Google search results, detect and remove invalid advertising traffic in Google Ads, and test algorithms and build models that power services like Google Analytics Intelligence that apply machine-learning to surface suggestions and insights for customers based on their analytics data and like Google Ads that applies broad models to

[11] Dynamic remarketing for web setup guide (available at https://support.google.com/google-ads/answer/6077124).

improve ads personalization and relevance. These capabilities are critical to the value of the products we deliver to customers today."[12] Thus, Google can have the capability to use the data it collects for understanding online behavior and trends, machine learning, and improving its own products and services.

2. TikTok Cookies

48. Defendant also causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users elect to reject all non-essential cookies, to and from the **analytics.tiktok.com** domain. This domain is associated with TikTok for Buisness, a suite of tools offered by TikTok, a social media platform owned by ByteDance Ltd., known for short-form video sharing. [13] The TikTok platform is used to create and share videos, and it utilizes cookies for various purposes including assisting brands and marketers to create, manage, and optimize ad campaigns on the platform.[14]

49. TikTok utilizes **analytics.tiktok.com** cookies to collect data on user interactions with websites that have integrated TikTok's tracking technologies (such as the Website). These cookies are used to "measure and improve the performance of your advertising campaigns and to personalize the user's experience (including ads) on TikTok."[15] TikTok further explains that it uses cookies to "match events with people who engage with your content on TikTok. Matched events are used to improve measurement and optimize ad campaigns. They can also contribute to building your retargeting and engagement audiences." *Id.* These cookies enable TikTok to recognize and track users across different sessions and domains (i.e., cross-site tracking) and to collect and synchronize user data to observe and evaluate TikTok user behavior.

---

[12] Shared Data Under Measurement Controller-Controller Data Protection Terms (available at https://support.google.com/analytics/answer/9024351).

[13] *See* Our advertising and measurement cookies (available at https://business.safety.google/adscookies/).

[14] *See, e.g.*, TikTok for Business (https://ads.tiktok.com/business/en-US/products/ads; and https://ads.tiktok.com/business/en-US/products/measurement); TikTok Business Help Center; Using Cookies with TikTok Pixel (available at https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en).

[15] TikTok Business Help Center; Using Cookies with TikTok Pixel (available at https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en).

50. These cookies enable TikTok to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, including *email addresses and phone numbers*; (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) session information, (x) user identifiers, and (xi) geolocation data in the form of the IP address.[16]

51. For example, the TikTok software code that Defendant causes to be stored on and executed by the Website user's device causes the following data to be sent to TikTok's domain, at https://analytics.tiktok.com/api/v2/monitor:

[REMAINDER OF PAGE INTENTIONALLY BLANK]

[16] *Id.*; *see also* TikTok for Business: Enhance Data Postback with the TikTok Pixel (https://ads.tiktok.com/help/article/enhance-data-postback-with-the-tiktok-pixel?lang=en); TikTok for Business: Advanced Matching for Web (available at https://ads.tiktok.com/help/article/advanced-matching-web?redirected=1); TikTok for Business: About TikTok Pixel (available at https://ads.tiktok.com/help/article/tiktok-pixel?lang=en).

```
{
  "metric_name": "pixel_send",
  "pixel_code": "C3NJENNB3D4L4OG53BP0",
  "platform": 0,
  "net_type": "4g",
  "app_name": "external",
  "placement": "non",
  "lib": {
    "lib_version": "2.1.33",
    "ttq_name": "ttq"
  },
  "in_iframe": 2,
  "time_to_last_start": 554,
  "time_to_navigation_start": 3164,
  "latency": 0,
  "page_url": "https://www.motorola.com/us/smartphones-thinkphone/p?skuId=869",
  "att_status": 3,
  "pageview_id": "pageId-1707536995331-3464495649027",
  "session_id": "505c337b-c7c7-11ee-b792-b8cef6a28284::GFrrbllzJ4oSVG2fVzLH",
  "variation_id": "test_2_dual_track",
  "ad_id": "undefined",
  "creative_id": "undefined",
  "partner": "non",
  "ext_json": {
    "performance": [],
    "pixel_list": "C3NJENNB3D4L4OG53BP0",
    "pixel_api_conflict_flag": false,
    "event": "Pageview"
  }
}
```


52. The data includes the "session_id," which is a unique identifier generated by TikTok to track a user's activity. This allows TikTok to correlate the user's behavior from a browsing session, including page views and conversions, to a particular user to enhance advertising measurement, attribution, and targeting.[17]

53. The data further indicates, among other things, that the user has viewed the page on the Defendant's website at the url https://www.motorola.com/us/smartphones-thinkphone/p?skuId=869.

54. Along with this data, the TikTok software code that Defendant causes to be stored on and executed by the user's device causes the "_ttp" cookie to be sent to TikTok's domain:

[17] *See, e.g.*, How to get TikTok session id? (available at https://gbtimes.com/how-to-get-tiktok-session-id/).

Key	Value
_ttp	2c6Hp7HGnbbbk0KZU9bB4SJC5ou

55. According to TikTok's documentation, the "_ttp" cookie is one of the company's advertising cookies, the purpose of which is "[t]o measure and improve the performance of your advertising campaigns and to personalize the user's experience (including ads) on TikTok."[18]

56. Further, along with all of this data, the TikTok software code that Defendant causes to be stored on and executed by the user's device causes the user's "user-agent" information to be sent to TikTok:

Key	Value
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

As discussed above with respect to Google, the "user-agent" corresponds to the device and browser that the user has used to access the Website. In this case, the user-agent value corresponds to Google's Chrome browser version 121, running on the Catalina version of macOS.[19]

57. Finally, the data sent to TikTok includes the user's IP address.

58. By collecting this user data, TikTok performs user behavior tracking, i.e., monitoring user actions like page views, clicks, and interactions to understand user engagement; advertising optimization, i.e., gathering data to enhance the relevance and effectiveness of

[18] *See* TikTok for Business: Using Cookies with TikTok Pixel (available at https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en).

[19] There are many tools on the web that are capable of parsing user-agent strings to determine what browser and operating system they pertain to. One such tool is located at https://explore.whatismybrowser.com/useragents/parse.

TikTok advertising campaigns; and performance measurement (i.e., assessing the success of marketing efforts by analyze user responses to ads and content).[20]

59. Further, TikTok's Automatic Advanced Matching feature functions as follows: "When a visitor lands on your website and inputs customer information during registration, sign-in, contact, or checkout on a website where you installed your pixel, Automatic Advanced Matching will capture information from those fields. …TikTok will use hashed information to link event information to people on TikTok. Tiktok may use matched events to better attribute events to TikTok ads, optimize advertisers' future campaigns, and depending on advertisers' and users' settings, TikTok may also add people to advertisers' retargeting or engagement audiences."[21]

3. Additional Third Party Cookies

60. Defendant also causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users elect to reject all non-essential cookies, to and from other domains, including (i) s.amazon-adsystem.com; (ii) events.release.narrativ.com; and (iii) gis.goinstore.com.

61. The **s.amazon-adsystem.com** domain is associated with Amazon's advertising services. Amazon utilizes cookies to collect data on user interactions with websites (including browsing behavior and preferences) to perform advertising and personalization functions, i.e., to assist Amazon in delivering advertisements tailored to user interests. Further, the cookies perform analytics functions to enable Amazon to measure and analyze the performance of its services and to ensure that ads are effective and relevant.

62. The subdomain **events.release.narrativ.com** is associated with Howl Technologies, Inc., a social commerce platform that enables brands to market their products with social media content creators. Howl uses these cookies to perform user authentication (i.e, verify

---

[20] *See* TikTok for Business: Using Cookies with TikTok Pixel (available at https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en).

[21] TikTok for Business: How to set up Automatic Advanced Matching (available at https://ads.tiktok.com/help/article/how-to-set-up-automatic-advanced-matching?lang=en).

user identities and track session information), analytics (i.e., track user interactions, such as clicks and impressions, to facilitate attribution and analytics for their services); and personalization (i.e., store user preferences and tailor the content presented based on user interactions).

63. The domain **gis.goinstore.com** is associated with Emplifi, Inc., a social media management platform for brands. Emplifi uses these cookies to perform session management, user authentication, analytics and performance tracking by collecting data on user interactions, and personalization.

64. These cookies allow these Third Parties to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) demographic information, (v) interests and preferences, (vi) shopping behaviors, (vii) device information, (viii) referring URLs, (ix) session information, (x) user identifiers, and (xi) geolocation data.

E. <u>The Private Communications Collected is Valuable.</u>

65. The Personal Communications that the Third Parties track and collect by way of the cookies on the Website is valuable to Defendant as well as the Third Parties. Defendant can use the data to create and analyze the performance of marketing campaigns, website design, product placement, and target specific users or groups of users for advertisements. For instance, if Defendant wanted to market certain of its consumer electronics to consumers, Defendant could use the data collected by the Third Parties to monitor users who visit webpages related to specific products, then advertise similar products to those particular users when they visit other webpages. The third-party cookies also enable Defendant to target online advertisements to users when they visit ***other*** websites, even those completely unrelated to Defendant and its products.

66. Data about users' browsing history enables Defendant to spot patterns in users' behavior on the Website and their interests in, among other things, Defendant's consumer electronics products. On a broader scale, it enables Defendant to gain an understanding of trends happening across its brands and across the consumer electronics market. All of this helps

Defendant further monetize its Website and maximize revenue by collecting and analyzing user data.

67. The value of the Private Communications tracked and collected by the Third Parties using cookies on the Website can be quantified. Legal scholars observe that "[p]ersonal information is an important currency in the new millennium."[22] Indeed, "[t]he monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend." *Id*. "Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information." *Id*.

68. Numerous empirical studies quantify the appropriate value measure for personal data. Generally, the value of personal data is measured as either the consumer's willingness to accept compensation to sell her data or the consumer's willingness to pay to protect her information.

69. Through its false representations and aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties to track users' Private Communications on the Website using third-party cookies, Defendant is unjustly enriching itself at the cost of consumer privacy and choice, when the consumer could otherwise have the ability to choose if and how they would monetize their data.

PLAINTIFF'S EXPERIENCES

70. Plaintiff visited the Website to browse information about Motorola's products on multiple occasions during the last four years, including, in or around February 2022, December 2022, November 2023, and January 2024.

71. When Plaintiff visited the Website, the Website immediately presented him with Defendant's popup cookie consent banner, which provided the option to select the "Click Here to Reject All non-essential cookies" link. Plaintiff viewed Defendant's representation on the popup cookie consent banner that, "We use cookies and similar technologies to personalize content and ads and analyze our traffic. By browsing our site or by selecting "X", you agree to

[22] *See* Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 Harv. L. Rev. 2055, 2056–57 (2004).

our use of cookies and our sharing of information with our partners." Plaintiff also viewed Defendant's additional representation that users could "Click Here to Reject All non-essential cookies."

72. Consistent with his typical practice in rejecting or otherwise declining the placement or use of cookies and tracking technologies, Plaintiff selected and clicked the "Click Here to Reject All non-essential cookies" link. Plaintiff believed that selecting the "Click Here to Reject All non-essential cookies" link on the popup cookie consent banner found on the Website would allow him to opt out of, decline, and/or reject all non-essential cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of tracking data to third-party advertising networks, analytics services, and/or social media companies for the purposes of providing personalized content, advertising, and analytics services).

73. In selecting the "Click Here to Reject All non-essential cookies" link Plaintiff gave Defendant notice that he did not consent to the use or placement of cookies and tracking technologies while browsing the Website. Further, Plaintiff specifically rejected, based on Defendant's representations, those cookies used to "personalize content and ads and analyze [Website] traffic" and share information with third parties. In reliance on these representations and promises, only then did Plaintiff continue browsing the Website.

74. Even before the popup cookie consent banner appeared on the screen, Defendant nonetheless caused cookies and tracking technologies, including those used for personalized content, advertising, analytics, and social media, to be placed on Plaintiff's device and/or transmitted to the Third Parties along with user data, without Plaintiff's knowledge. Accordingly, the popup cookie consent banner's representation to Plaintiff that he could reject the use and/or placement of all non-essential cookies and tracking technologies while he browsed the Website was false. Contrary to what Defendant made Plaintiff believe, he did not have a choice about whether third-party cookies would be placed on his device and/or transmitted to the Third Parties along with his user data; rather, Defendant had already caused that to happen.

75. Then, as Plaintiff continued to browse the Website in reliance on the promises Defendant made in the cookie consent banner, and despite Plaintiff's clear rejection of the use and/or placement of such cookies and tracking technologies, Defendant nonetheless continued to cause the placement and/or transmission of cookies along with user data, including those involved in providing personalized content, advertising, analytics, and social media content from the Third Parties on his device. In doing so, Defendant permitted the Third Parties to track and collect Plaintiff's Private Communications as Plaintiff browsed the Website.

76. Defendant's representations that consumers could "Reject All non-essential cookies" while Plaintiff and users browsed the Website, or at least those involved in providing personalized content, advertising, and social media services, were untrue. Had Plaintiff known this fact, he would not have used the Website. Moreover, Plaintiff reviewed the popup cookie consent banner and Privacy Statement prior to using the Website. Had Defendant disclosed that it would continue to cause cookies and tracking technologies to be stored on consumers' devices even after they choose to reject all non-essential cookies, Plaintiff would have noticed it and would not have used the Website or, at a minimum, he would have interacted with the Website differently.

77. Plaintiff continues to desire to browse content featured on the Website. Plaintiff would like to browse websites that do not misrepresent that users can reject all non-essential cookies and tracking technologies. If the Website were programmed to honor users' requests to reject all non-essential cookies and tracking technologies, Plaintiff would likely browse the Website again in the future, but will not do so until then. Plaintiff regularly visits websites that feature content similar to that of the Website. Because Plaintiff does not know how the Website is programmed, which can change over time, and because he does not have the technical knowledge necessary to test whether the Website honors users' requests to reject all non-essential cookies and tracking technologies, Plaintiff will be unable to rely on Defendant's representations when browsing the Website in the future absent an injunction that prohibits Defendant from making misrepresentations on the Website. The only way to determine what

network traffic is sent to third parties when visiting a website is to use a specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed for use by "developers" (i.e., software developers), whose specialized training enables them to analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff is not a software developer and has not received training with respect to HTTP network calls.

CLASS ALLEGATIONS

78. Plaintiff brings this Class Action Complaint on behalf of himself and a proposed class of similarly situated persons, pursuant to Rules 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure. Plaintiff seeks to represent the following group of similarly situated persons, defined as follows:

Class: All persons who browsed the Website in the State of California after clicking the "Reject All" button in the popup cookies consent banner within the four years preceding the filing of this Complaint (the "Class Period").

79. This action has been brought and may properly be maintained as a class action against Defendant because there is a well-defined community of interest in the litigation and the proposed class is easily ascertainable.

80. **Numerosity:** Plaintiff does not know the exact size of the Class, but he estimates that it is composed of more than 100 persons. The persons in the Class are so numerous that the joinder of all such persons is impracticable and the disposition of their claims in a class action rather than in individual actions will benefit the parties and the courts.

81. **Common Questions Predominate:** This action involves common questions of law and fact to the Class because each class member's claim derives from the same unlawful conduct that led them to believe that Defendant would not cause third-party cookies to be placed on their browsers and devices and/or transmitted to third parties along with user data, after Class members chose to reject all non-essential cookies and tracking technologies on the Website, nor would Defendant permit third parties to track and collect Class members' Private Communications as Class members browsed the Website.

82. The common questions of law and fact predominate over individual questions, as proof of a common or single set of facts will establish the right of each member of the Class to recover. The questions of law and fact common to the Class are:

a. Whether Defendant's actions violate California laws invoked herein; and

b. Whether Plaintiff and Class members are entitled to damages, restitution, injunctive and other equitable relief, reasonable attorneys' fees, prejudgment interest and costs of this suit.

83. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, Plaintiff, like the other Class members, visited the Website, rejected non-essential cookies, and had his confidential Private Communications intercepted by the Third Parties.

84. **Adequacy of Representation:** Plaintiff will fairly and adequately protect the interests of all Class members because it is in his best interests to prosecute the claims alleged herein to obtain full compensation due to him for the unfair and illegal conduct of which he complains. Plaintiff also has no interests in conflict with, or antagonistic to, the interests of Class members. Plaintiff has retained highly competent and experienced class action attorneys to represent his interests and those of the Class. By prevailing on his claims, Plaintiff will establish Defendant's liability to all Class members. Plaintiff and his counsel have the necessary financial resources to adequately and vigorously litigate this class action, and Plaintiff and counsel are aware of their fiduciary responsibilities to the Class members and are determined to diligently discharge those duties by vigorously seeking the maximum possible recovery for Class members.

85. **Superiority:** There is no plain, speedy, or adequate remedy other than by maintenance of this class action. The prosecution of individual remedies by members of the Class will tend to establish inconsistent standards of conduct for Defendant and result in the impairment of Class members' rights and the disposition of their interests through actions to which they were not parties. Class action treatment will permit a large number of similarly

situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would engender. Furthermore, as the damages suffered by each individual member of the Class may be relatively small, the expenses and burden of individual litigation would make it difficult or impossible for individual members of the class to redress the wrongs done to them, while an important public interest will be served by addressing the matter as a class action. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

First Cause of Action: Invasion of Privacy

86. Plaintiff realleges and incorporates the paragraphs of this Complaint as if set forth herein.

87. To plead an invasion of privacy claim, Plaintiff must show an invasion of (i) a legally protected privacy interest; (ii) where Plaintiff had a reasonable expectation of privacy in the circumstances; and (iii) conduct by Defendant constituting a serious invasion of privacy.

88. Defendant has intruded upon the following legally protected privacy interests of Plaintiff and Class members: (i) the California Invasion of Privacy Act, as alleged herein; (ii) the California Constitution, which guarantees Californians the right to privacy; (iii) the California Wiretap Acts as alleged herein; (iv) Cal. Penal Code § 484(a), which prohibits the knowing theft or defrauding of property "by any false or fraudulent representation or pretense;" and (v) Plaintiff's and Class members' Fourth Amendment right to privacy.

89. Plaintiff and Class members had a reasonable expectation of privacy under the circumstances, as Defendant affirmatively promised users they could "Click Here to Reject All non-essential cookies" and tracking technologies before proceeding to browse the Website. Plaintiff and other Class members directed their electronic devices to access the Website and, when presented with the popup cookies consent banner on the Website, Plaintiff and Class members rejected non-essential cookies and reasonably expected that his and their rejection of

non-essential cookies and tracking technologies would be honored. That is, he and they reasonably believed that Defendant would not permit the Third Parties to store and send cookies and/or use other such tracking technologies on their devices while they browsed the Website. Plaintiff and Class members also reasonably expected that, if they rejected such cookies and/or tracking technologies, Defendant would not permit the Third Parties to track and collect Plaintiff's and Class members' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, on the Website.

90. Such information is "personal information" under California law, which defines personal information as including "Internet or other electronic network activity information," such as "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

91. Defendant, in violation of Plaintiff's and other Class members' reasonable expectation of privacy and without their consent, permits the Third Parties to use cookies and other tracking technologies to collect, track, and compile users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data. The data that Defendant allowed third parties to collect enables the Third Parties to, *inter alia*, create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics; create audience segments based on shared traits (such as millennials, tech enthusiasts, etc.); and perform targeted advertising and marketing analytics. Further, the Third Parties share user data and/or the user profiles to unknown parties to further their financial gain. The consumer profiles are and can be used to further invade Plaintiff's and users' privacy, by allowing third parties to learn intimate details of their lives, and target them for advertising and other purposes, as

described herein, thereby harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them.

92. Defendant's actions constituted a serious invasion of privacy in that it invaded a zone of privacy protected by the Fourth Amendment (i.e., one's personal communications), and violated criminal laws on wiretapping and invasion of privacy. These acts constitute an egregious breach of social norms that is highly offensive.

93. Defendant's intrusion into Plaintiff's privacy was also highly offensive to a reasonable person.

94. Defendant lacked a legitimate business interest in causing the placement and/or transmission of third-party cookies along with user data that allowed the Third Parties to track, intercept, receive, and collect Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, without their consent.

95. Plaintiff and Class members have been damaged by Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

96. Plaintiff and Class members seeks appropriate relief for that injury, including but not limited to, damages that will compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff's and Class members' privacy.

97. Plaintiff and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights and Plaintiff's and Class members' rejection of the Website's use of non-essential cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Second Cause of Action: Intrusion Upon Seclusion

98. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

99. To assert a claim for intrusion upon seclusion, Plaintiff must plead (i) that Defendant intentionally intruded into a place, conversation, or matter as to which Plaintiff had a reasonable expectation of privacy; and (ii) that the intrusion was highly offensive to a reasonable person.

100. By permitting third-party cookies to be stored on consumers' devices without consent, which enabled the Third Parties to track and collect Plaintiff's and Class members' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, in violation of Defendant's representations otherwise in the popup cookie consent banner, Defendant intentionally intruded upon the solitude or seclusion of Website users. Defendant effectively placed the Third Parties in the middle of communications to which they were not invited, welcomed, or authorized.

101. The Third Parties' tracking and collecting of Plaintiff's and Class member's Private Communications on the Website using third-party cookies that Defendant caused to be stored on users' devices—and to be transmitted to Third Parties—was not authorized by Plaintiff and Class members, and, in fact, those Website users specifically chose to "Reject All non-essential cookies."

102. Plaintiff and the Class members had an objectively reasonable expectation of privacy surrounding his and their Private Communications on the Website based on Defendant's promise that users could "Reject All non-essential cookies", as well as state criminal and civil laws designed to protect individual privacy.

103. Defendant's intentional intrusion into Plaintiff's and other users' Private Communications would be highly offensive to a reasonable person given that Defendant represented that Website users could "Reject All non-essential cookies" when, in fact, Defendant caused such third-party cookies to be stored on consumers' devices and browsers, and to be transmitted to third parties, even when consumers rejected all such cookies. Indeed, Plaintiff and

Class members reasonably expected, based on Defendant's false representations, that when he and they rejected all non-essential cookies and tracking technologies, Defendant would not cause such third-party cookies to be stored on his and their devices or permit the Third Parties to obtain their Private Communications on the Website, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

104. Defendant's conduct was intentional and intruded on Plaintiff's and users' Private Communications on the Website.

105. Plaintiff and Class members have been damaged by Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

106. Plaintiff and Class members seeks appropriate relief for that injury, including but not limited to, damages that will compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff's and Class members' privacy.

107. Plaintiff and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights and Plaintiff's and Class members' rejection of the Website's use of non-essential cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

<u>Third Cause of Action</u>: Wiretapping in Violation of the California Invasion of Privacy Act (California Penal Code § 631)

108. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

109. California Penal Code § 631(a) provides, in pertinent part:

> "Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so

> obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars . . . ."

110. The California Supreme Court has repeatedly stated an "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line permits an outsider to tap his telephone or listen in on the call." *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added).

111. Further, as the California Supreme Court has held, in explaining the legislative purpose behind CIPA:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and *its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.*
>
> As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication— the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas, 38 Cal. 3d at 360-61 (emphasis supplied; internal citations omitted).

112. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under § 631(a), Plaintiff need only establish that Defendant, "by means of any machine, instrument, contrivance, or in any other manner," did ***any*** of the following:

> [i] Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;
>
> [ii] Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;
>
> [iii] Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained

Cal. Penal Code § 631(a).

113. CIPA § 631(a) also penalizes those who [iv] "aid[], agree[] with, employ[], or conspire[] with any person" who conducts the aforementioned wiretapping, or those who "permit" the wiretapping.

114. Defendant is a "person" within the meaning of California Penal Code § 631.

115. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *see also Bradley v. Google, Inc.*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications.").

116. The Third Parties' cookies—as well as the software code of the Third Parties responsible for placing the cookies and transmitting data from user devices to the Third Parties—constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA (and, even if they do not, Defendant's deliberate and purposeful scheme that facilitated the interceptions falls under the broad statutory catch-all category of "any other manner").

117. Each of the Third Parties is a "separate legal entity that offers [a] 'software-as-a-service' and not merely a passive device." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, the Third Parties had the capability to use the wiretapped information for their own purposes and, as alleged above, they did in fact use the wiretapped information for their own business purposes. Accordingly, the Third Parties were third parties to any communication between Plaintiff and Class members, on the one hand, and Defendant, on the other. *Id.* at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

118. Under § 631(a), Defendant must show it had the consent of all parties to a communication.

119. At all relevant times, the Website caused Plaintiff and Class members' browsers to store the Third Parties' cookies and to transmit those cookies alongside Private Communications—including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—to the Third Parties without Plaintiff's and Class members' consent. By configuring the Website in this manner, Defendant willfully aided, agreed with, employed, permitted, or otherwise enabled the Third Parties to wiretap Plaintiff and Class members using the Third Parties' cookies and to accomplish the wrongful conduct alleged herein.

120. At all relevant times, by their cookies and corresponding software code, the Third Parties willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, attempted to read, and/or learned the contents or meaning of electronic communications of Plaintiff and Class members, on the one hand, and Defendant, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

121. The Private Communications of Plaintiff and Class members, on the one hand, and Defendant, on the other, that the Third Parties automatically intercepted directly communicates the Website user's affirmative decisions, actions, choices, preferences, and activities, which constitute the "contents" of electronic communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

122. At all relevant times, the Third Parties used or attempted to use the Private Communications automatically intercepted by their cookie tracking technologies for their own purposes.

123. Plaintiff and Class members did not provide their prior consent to the Third Parties' intentional access, interception, reading, learning, recording, collection, and usage of

Plaintiff's and Class members' electronic communications. Nor did Plaintiff and Class members provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties' conduct. On the contrary, Plaintiff and Class members expressly declined to allow Third Parties' cookies and tracking technologies to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' electronic communications by choosing to reject non-essential cookies in the consent banner.

124. The wiretapping of Plaintiff and Class members occurred in California, where Plaintiff and Class members accessed the Website and where the Third Parties—as enabled by Defendant—routed Plaintiff's and Class members' electronic communications to Third Parties' servers. Among other things, the cookies, as well as the software code responsible for placing the cookies and transmitting them and other Private Communications to the Third Parties, resided on Plaintiff's California-located device. In particular, the user's California-based device, after downloading the software code from the Third Parties' servers, (i) stored the code onto the user's disk; (ii) converted the code into machine-executable format; and (iii) executed the code, causing the transmission of data (including cookie data) to and from the Third Parties.

125. Plaintiff and Class members have suffered loss by reason of these violations, including, but not limited to, (i) violation of his and their right to privacy, (ii) loss of value in his and their Private Communications, (iii) damage to and loss of Plaintiff's and Class members' property right to control the dissemination and use of their Private Communications, and (iv) loss of their Private Communications to the Third Parties with no consent.

126. Pursuant to California Penal Code § 637.2, Plaintiff and Class members have been injured by the violations of California Penal Code § 631, and each seeks statutory damages of the greater of $5,000, or three times the amount of actual damages, for each of Defendant's violations of CIPA § 631(a), as well as injunctive relief.

127. Unless enjoined, Defendant will continue to commit the illegal acts alleged herein including, but not limited to, permitting third parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' electronic Private Communications with

Defendant. Plaintiff, Class members, and the general public continue to be at risk because Plaintiff, Class members, and the general public frequently use the internet to search for information and content related to consumer electronics products. Plaintiff, Class members, and the general public continue to desire to use the internet for that purpose. Plaintiff, Class members, and the general public have no practical way to know if his and their request to reject non-essential cookies and tracking technologies will be honored and/or whether Defendant will permit third parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' electronic Private Communications with Defendant. Further, Defendant has already permitted the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' electronic Private Communications with Defendant and will continue to do so unless and until enjoined.

Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of Privacy Act (California Penal Code § 638.51)

128. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

129. The California Invasion of Privacy Act, codified at Cal. Penal Code §§ 630 to 638, includes the following statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

130. California Penal Code Section 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

131. A "pen register" is a "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

132. The Third Parties' cookies and the corresponding software code installed by Defendant on its Website are each "pen registers" because they are "device[s] or process[es]" that "capture[d]" the "routing, addressing, or signaling information"—including, the IP address and user-agent information—from the electronic communications transmitted by Plaintiff's and the Class's computers or devices. Cal. Penal Code § 638.50(b).

133. At all relevant times, Defendant caused the Third Parties' cookies and the corresponding software code—which are pen registers—to be placed on Plaintiff's and Class members' browsers and devices, and/or to be used to transmit Plaintiff's and Class members' IP address and user-agent information. *See Greenley v. Kochava,* 2023 WL 4833466, at *15-16 (S.D. Cal. July 27, 2023); *Shah v. Fandom, Inc.*, 2024 U.S. Dist. LEXIS 193032, at *5-11 (N.D. Cal. Oct. 21, 2024).

134. Some of the information collected by the Third Parties' cookies and the corresponding software, including IP addresses and user-agent information, does not constitute the content of Plaintiff's and the Class members' electronic communications with the Website. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1008 (9th Cir. 2014). ("IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication…") (cleaned up).

135. Plaintiff and Class members did not provide their prior consent to Defendant's use of third-party cookies and the corresponding software. On the contrary, Plaintiff and the Class members informed Defendant that they did not consent to the Website's use of third-party cookies by clicking the "Reject All non-essential cookies" link in the cookie consent banner.

136. Defendant did not obtain a court order to install or use the third-party cookies and corresponding software to track and collect Plaintiff's and Class member's IP addresses and user-agent information.

137. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members suffered losses and were damaged in an amount to be determined at trial.

138. Pursuant to Penal Code § 637.2(a)(1), Plaintiff and Class members are also entitled to statutory damages of $5,000 for each of Defendant's violations of § 638.51(a).

Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation

139. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

140. Defendant fraudulently and deceptively informed Plaintiff and Class members that he and they could "Click Here to Reject All non-essential cookies."

141. However, despite Defendant's representations otherwise, Defendant caused third-party cookies and software code to be stored on consumers' devices, and to be transmitted to the Third Parties alongside Private Communications, even after users clicked the "Click Here to Reject All non-essential cookies" link in the popup cookie consent banner. These cookies and corresponding software code allowed the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiff's and Class members' Private Communications, even when consumers had previously chosen to "Reject All non-essential cookies."

142. These misrepresentations and omissions were known exclusively to, and actively concealed by Defendant, not reasonably known to Plaintiff and Class members, and material at the time they were made. Defendant knew, or should have known, how the Website functioned, including the Third Party's resources it installed on the Website and the third-party cookies in use on the Website, through testing the Website, evaluating its performance metrics by means of its accounts with the Third Parties, or otherwise, and knew, or should have known, that the Website's programming allowed the third-party cookies to be placed on users'—including Plaintiff's—browsers and devices and/or transmitted to the Third Parties along with users' Private Communications even after users attempted to "Reject All non-essential cookies", which Defendant promised its users they could do. Defendant's misrepresentations and omissions concerned material facts that were essential to the analysis undertaken by Plaintiff and Class members as to whether to use the Website. In misleading Plaintiff and Class members and not so informing him and them, Defendant breached its duty to Plaintiff and Class members. Defendant also gained financially from, and as a result of, its breach.

143. Plaintiff and Class members relied to their detriment on Defendant's misrepresentations and fraudulent omissions.

144. Plaintiff and Class members have suffered an injury-in-fact, including the loss of money and/or property, as a result of Defendant's unfair, deceptive, and/or unlawful practices, including the unauthorized interception of his and their Personal Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, which have value as demonstrated by the use and sale of consumers' browsing activity, as alleged above. Plaintiff and Class members have also suffered harm in the form of diminution of the value of his and their private and personally identifiable information and communications.

145. Defendant's actions caused damage to and loss of Plaintiff's and Class members' property right to control the dissemination and use of their personal information and communications.

146. Defendant's representation that consumers could reject non-essential cookies (including "cookies and similar technologies [used] to personalize content and ads and analyze our traffic") if they clicked the "Click Here to Reject All non-essential cookies" link was untrue. Again, had Plaintiff and Class members known these facts, they would not have used the Website. Moreover, Plaintiff and Class members reviewed the popup cookie consent banner and Privacy Statement prior to their interactions with the Website. Had Defendant disclosed that it caused third-party non-essential cookies to be stored on Website visitors' devices that are related to personalization, advertising, analytics, and social media and/or share information with third parties even after they choose to reject all such non-essential cookies, Plaintiff and Class members would have noticed it and would not have interacted with the Website.

147. By and through such fraud, deceit, misrepresentations and/or omissions, Defendant intended to induce Plaintiff and Class members to alter their positions to their detriment. Specifically, Defendant fraudulently and deceptively induced Plaintiff and Class

members to, without limitation, use the Website under the mistaken belief that Defendant would not permit third parties to obtain users' Private Communications when consumers chose to reject non-essential cookies. As a result, Plaintiff and the Class provided more personal data than they would have otherwise.

148. Plaintiff and Class members justifiably and reasonably relied on Defendant's misrepresentations and omissions, and, accordingly, were damaged by Defendant's conduct.

149. As a direct and proximate result of Defendant's misrepresentations and/or omissions, Plaintiff and Class members have suffered damages, as alleged above, and are entitled to just compensation, including monetary damages.

150. Plaintiff and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights and Plaintiff's and Class members' rejection of the Website's use of non-essential cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Sixth Cause of Action: Unjust Enrichment

151. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

152. Defendant created and implemented a scheme to increase its own profits through a pervasive pattern of false statements and fraudulent omissions.

153. Defendant was unjustly enriched as a result of its wrongful conduct, including through its misrepresentation that users could "Reject All non-essential cookies" and by permitting the Third Parties to store and transmit cookies on Plaintiff's and Class members' devices and browsers, which permitted the Third Parties to track and collect users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even after Class members rejected such cookies.

154. Plaintiff and Class members' Personal Communications have conferred an economic benefit on Defendant.

155. Defendant has been unjustly enriched at the expense of Plaintiff and Class members, and Defendant has unjustly retained the benefits of its unlawful and wrongful conduct.

156. Defendant appreciated, recognized, and chose to accept the monetary benefits that Plaintiff and Class members conferred onto Defendant at his and their detriment. These benefits were the expected result of Defendant acting in its pecuniary interest at the expense of Plaintiff and Class members.

157. It would be unjust for Defendant to retain the value of Plaintiff's and Class members' property and any profits earned thereon.

158. There is no justification for Defendant's enrichment. It would be inequitable, unconscionable, and unjust for Defendant to be permitted to retain these benefits because the benefits were procured as a result of its wrongful conduct.

159. Plaintiff and Class members are entitled to restitution of the benefits Defendant unjustly retained and/or any amounts necessary to return Plaintiff and Class members to the position he and they occupied prior to having his and their Private Communications tracked and collected by the Third Parties.

160. Plaintiff pleads this claim separately, as well as in the alternative, to his other claims, as without such claims Plaintiff would have no adequate legal remedy.

Seventh Cause of Action: Breach of Contract

161. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

162. Defendant's relationship with its users is governed by the Website's Privacy Statement, which explains:

> Your privacy is important to Motorola. This privacy statement applies to data collected through websites owned and operated by Motorola Mobility LLC, a Lenovo company, ("Motorola") and certain offline services maintained by Motorola or our service providers and partners. This statement describes the information practices for Motorola websites including, but not limited to, www.motorola.com and support.motorola.com This privacy statement describes the information practices for Motorola websites, including what types of information are collected, how Motorola uses information and

> for what purposes; with whom information is shared; and how Motorola protects information. It also describes your choices regarding use, access, correction and deletion of your personal information, among other topics. In addition, this statement addresses personal information collection and use by Motorola in certain other (including offline) contexts, such as marketing, newsletters, events, and customer service and support.

163. The Website's Privacy Statement contains enforceable promises that Defendant made to Plaintiff and Class members, including, but not limited to, the following provisions:

- Where required by applicable law, Motorola will acquire consent from you prior to using certain cookies during your Motorola website experience and/or will offer you the opportunity to choose which types of cookies to enable or disable.

- Motorola and its service providers, including Google and DoubleClick, use cookies to report how your ad impressions, other uses of ad services, and interactions with these ad impressions and ad services are related to visits to our website. If you do not want to have this information used for serving you interest-based ads, you may opt-out by following the steps below.

- However, if you prefer not to store cookies, you can choose to...Utilize the cookie consent and control options offered by a Motorola website (if available and as required by applicable law)[.]

164. Defendant breached these duties and violated these promises by causing third-party cookies to be stored on consumers' devices and browsers that enabled the Third Parties to track and collect Plaintiff's and Class member's Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even though Defendant represented that Plaintiff and other users could "Reject All non-essential cookies". Plaintiff and Class members, in fact, chose to reject such cookies by selecting the "Click Here to Reject All non-essential cookies" link.

165. At all relevant times and in all relevant ways, Plaintiff and Class members performed his and their obligations under the Privacy Statement or were excused from performance of such obligations through the unknown and unforeseen conduct of others.

166. Defendant's conduct in permitting the Third Parties to track and collect the Private Communications of Website users who chose to reject all cookies and tracking

technologies evaded the spirit of the bargain made between Defendant and Plaintiff and Class members since it caused Plaintiff and Class members to surrender more data than they had otherwise bargained for.

167. As a direct and proximate result of Defendant's breach of contract, Plaintiff and Class members did not receive the full benefit of the bargain, and instead received services from Defendant that were less valuable than described in the Privacy Statement. Plaintiff and Class members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendant's partial, deficient, and/or defective performance.

168. As a direct consequence of the breaches of contract and violations of promises described above, Plaintiff and Class members seek nominal damages, general damages, compensatory damages, consequential damages, unjust enrichment, and any other just relief.

Eighth Cause of Action: Breach of Implied Covenant of Good Faith and Fair Dealing

169. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

170. Defendant's relationship with its users is governed by the Website's Privacy Statement, which explains:

> Your privacy is important to Motorola. This privacy statement applies to data collected through websites owned and operated by Motorola Mobility LLC, a Lenovo company, ("Motorola") and certain offline services maintained by Motorola or our service providers and partners. This statement describes the information practices for Motorola websites including, but not limited to, www.motorola.com and support.motorola.com This privacy statement describes the information practices for Motorola websites, including what types of information are collected, how Motorola uses information and for what purposes; with whom information is shared; and how Motorola protects information. It also describes your choices regarding use, access, correction and deletion of your personal information, among other topics. In addition, this statement addresses personal information collection and use by Motorola in certain other (including offline) contexts, such as marketing, newsletters, events, and customer service and support.

171. The Website's Privacy Statement contains enforceable promises that Defendant made to Plaintiff and Class members, including, but not limited to, the following provisions:

- Where required by applicable law, Motorola will acquire consent from you prior to using certain cookies during your Motorola website experience and/or

> will offer you the opportunity to choose which types of cookies to enable or disable.
>
> - Motorola and its service providers, including Google and DoubleClick, use cookies to report how your ad impressions, other uses of ad services, and interactions with these ad impressions and ad services are related to visits to our website. If you do not want to have this information used for serving you interest-based ads, you may opt-out by following the steps below.
>
> - However, if you prefer not to store cookies, you can choose to...Utilize the cookie consent and control options offered by a Motorola website (if available and as required by applicable law)[.]

172. Defendant breached these duties and violated these promises by causing third-party cookies to be stored on consumers' devices and browsers that enabled the Third Parties to track and collect Plaintiff's and Class member's Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even though Defendant represented that Plaintiff and other users could reject all non-essential cookies and tracking technologies.] Plaintiff and Class members, in fact, chose to reject such cookies by selecting the "Click Here to Reject All non-essential cookies" link. California law recognizes the implied covenant of good faith and fair dealing in every contract.

173. In dealing between Defendant and its Website users, Defendant is invested with discretionary power affecting the rights of its users.

174. Defendant purports to respect and protect its Website users' privacy.

175. Despite their contractual promises to allow consumers to reject all non-essential cookies and other tracking technologies, Defendant took actions outside that contractual promise to deprive consumers, including Plaintiff and other users similarly situated, of benefits of their contract with Defendant.

176. Defendant's allowance of third parties to track and collect Website users' Private Communications with Defendant was objectively unreasonable given its privacy promises.

177. Defendant's conduct in permitting third parties to track and collect the Private Communications of Website users who chose to reject all non-essential cookies and tracking

technologies evaded the spirit of the bargain made between Defendant and Plaintiff and Class members since it caused Plaintiff and Class members to surrender more data than they had otherwise bargained for.

178. As a result of Defendant's misconduct and breach of its duty of good faith and fair dealing, Plaintiff and Class members suffered damages. Plaintiff and Class members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of providing their personal information, which, as alleged above, has ascertainable value.

179. As a direct consequence of the breach of the implied covenant of good faith and fair dealing described above, Plaintiff and Class members seek nominal damages, general damages, compensatory damages, consequential damages, and any other just relief.

Ninth Cause of Action: Trespass to Chattels

180. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

181. Defendant, intentionally and without consent or other legal justification, caused cookies to be stored on Plaintiff's and Class members' browsers and devices, which enabled the Third Parties and Defendant to track and collect Plaintiff's and Class members' Private Communications and use the data collected for their own advantage, as described above.

182. Defendant was unjustly enriched as a result of its wrongful conduct, including through its misrepresentation that users could reject all non-essential cookies and tracking technologies, and through their failure to disclose that Defendant causes third-party cookies to be stored on consumers' devices and browsers, which cause the Third Parties and Defendant to track and collect Plaintiff's and Class members' Private Communications even after consumers chose to reject such cookies.

183. Defendant intentionally caused third party software code to be stored onto Plaintiff's and Class members' devices, knowing that the code would be executed by those devices. The software code then placed and/or transmitted cookies along with Plaintiff's and Class members' Private Communications to the Third Parties. These intentional acts interfered

with Plaintiff's and Class members' use of the following personal property owned, leased, or controlled by Plaintiff and other users: (a) her and their computers and other electronic devices; and (b) her and their personally identifiable information.

184. Defendant's trespass of Plaintiff's and other users' computing devices resulted in harm to Plaintiff and other users and caused Plaintiff and other users the following damages:

a. Nominal damages for trespass;

b. Reduction of storage, disk space, and performance of Plaintiff's and other users' computing devices; and

c. Loss of value of Plaintiff's and other users' computing devices.

PRAYER FOR RELIEF

WHEREFORE, reserving all rights, Plaintiff, on behalf of himself and the Class members, respectfully requests judgment against Defendant as follows:

A. Certification of the proposed Class, including appointment of Plaintiff's counsel as class counsel;

B. An award of compensatory damages, including statutory damages where available, to Plaintiff and Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, including both pre- and post-judgment interest thereon;

C. An award of punitive damages;

D. An award of nominal damages;

E. An order for full restitution;

F. An order requiring Defendant to disgorge revenues and profits wrongfully obtained;

G. An order temporarily and permanently enjoining Defendant from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

H. For reasonable attorneys' fees and the costs of suit incurred; and

I. For such further relief as may be just and proper.

J.

Dated: December 31, 2024

GUTRIDE SAFIER LLP

/s/Seth A. Safier/s/

Seth A. Safier (State Bar No. 197427)
seth@gutridesafier.com
Marie A. McCrary (State Bar No. 262670)
marie@gutridesafier.com
Todd Kennedy (State Bar No. 250267)
todd@gutridesafier.com
Kali R. Backer (State Bar No. 342492)
kali@gutridesafier.com
100 Pine Street, Suite 1250
San Francisco, CA 94111
Telephone: (415) 639-9090
Facsimile: (415) 449-6469

Attorneys for Plaintiff